The Importance of Cyber Incident Response Plans and How to Create Them

By Kalie Pritchett*

June 2017

IMAGE VIA FLICKR

I. Consumers are Concerned about their Data.

A recent IDC survey found 84 percent of U.S. consumers are concerned about the privacy of their personal information, with 70 percent saying their concern is greater today than it was a few years ago.[1] With the influx of reports about data breaches and cyber-attacks of organizations, it is no surprise that the average American consumer is concerned about his or her personally-identifiable information being compromised.

The IDC survey also found that if directly affected by the breach, 78 percent of consumers said they would take their business elsewhere.[2] The impact of cyber-attacks on organizations, if not properly remedied, can result in great sums of money being paid out, loss of the company's customer base, and loss of investor confidence in the company's management.[3]

For example, one global company that suffered a large breach spent over $100 million on investigating the incident and on other direct remediation activities. But those costs were small compared with the subsequent multibillion-dollar loss in market capitalization, which was largely attributed to investors' loss of confidence in the company's ability to respond.[4]

With the potential detrimental losses to organizations, it is important for businesses to create, implement, and update cybersecurity measures to keep their customers' data safe.

II. Cyber Incident Response Plans – What are they?

While cyber-attacks and data breaches are arguably inevitable for businesses, there are ways to mitigate the damage caused by cyber-attacks. The best way to lower the cost per unit compromised is by creating and implementing a Cyber Incident Response Plan. Cyber Incident Response Plans are blueprints that help manage cybersecurity events in ways that limit damage, increase the confidence of investors (and customers), and reduce the recovery time and costs from the breach.[5] These Plans establish roles and responsibilities of employees, detail immediate remedial steps to be taken, and lay out the investigation, communication, and notification procedures to follow in the event of a breach. [6]

In AT&T's latest Cybersecurity Insights report, 62 percent of organizations acknowledged they were breached in 2015.[7] Only 34 percent of those organizations believe they have an effective Incident Response Plan.[8] Digital McKinsey highlights three common problems they have encountered in organizations' Incident Response Plans:

1. The documentation of how to act in the event of a breach is out of date. [9]
2. The plans, especially in global organizations, are not integrated across business units.[10]
3. Decision-making in a response scenario is often based on tribal knowledge and existing relationships. For example, many organizations will identify one or two "go to" people who should guide the organization in the event of a cyber incident. This may result in catastrophe if the "go to" person is unavailable during the breach.[11]

These pitfalls can be easily avoided by following the tips below.

III. Best Practices in creating Cyber Incident Response Plans

A good starting place for guidance in drafting a Cyber Incident Response Plan is the National Institute for Standards and Technology (NIST). The NIST defines five functions that should be included in cybersecurity programs: Identify, Protect, Detect, Respond, and Recover.[12] Cyber Incident Response Plans fall within the "Respond" section, and within the Plan, there should be tools to accomplish the four other functions NIST considers to analyze cyber incidents: identify, prevent, detect, and recover.[13]

- "Identify" refers to whether, and how quickly, the company identified the breach. Data classification, asset management, and risk management protocols can help organizations quickly identify cyber-attacks.[14]
- "Prevent" refers to whether the company has measures to prevent breaches. Asset control, employee training, and information management can lessen the probability of a breach.[15]
- "Detect" refers to whether they have measures to detect a breach. Companies' IT departments should have software installed to detect attacks on their systems.[16]
- "Recover" refers to whether the company has measures to recover the stolen or breached information.[17]

The best practice is to make sure that the company's Cyber Incident Response Plan has measures to prevent, detect, and recover information

that has been identified as a target for cyber criminals.

Digital McKinsey identifies four steps to make an Incident Response Plan:

1. Understand the current environment and plans in place;
2. Identify the most critical information assets your company has;
3. Create the plan and supporting tools with relevant people in your organization;
4. Integrate the plan into business processes.[18]

Before creating a written version of a Cyber Incident Response Plan, personnel from the legal department, IT department, C-suite, and other relevant departments should be assembled to brainstorm the following: the most critical data, the risks to that data, and ways to recover the data if breached.[19] After those have been identified, a written version of the company's Cyber Incident Response Plan should be created.

The following should be included in a Cyber Incident Response Plan:

- Clearly defined roles for employees,
- Immediate remedial steps to be taken to mitigate the damage (as determined by IT),
- A list of third party resources to contact (Cyber Insurance agent, IT specialists, crisis management specialists, and outside law firms),
- A course for investigating the incident,
- Up-to-date notification standards to determine if notification is required,
- A communication plan for press releases (templates, scripts, and designated person),
- Scheduled "fire drills" or table-top exercises to practice implementing the Plan to determine weaknesses.[20]

CSO Online cited four themes to improve cyber incident response:

First, acknowledge the unavoidable – a breach will likely happen.[21] Chuck Brooks, Vice President at Sutherland Global Services stated, "Breaches can happen and likely will happen sooner than later."[22] "A more rounded and integrated approach to developing effective incident response plans is needed, and this should cover a hybrid security position combining testing of physical security, human factors, and an organization's digital exposure," says Mike Loginov, CIO, CISO, and CEO at Ascot Barclay Cyber Security Group.[23]

Second, build the right team.[24] The IT department should not be the only part of the company involved in cybersecurity.[25] "Post-breach response is often an all-hands-on-deck affair. The C-suite, IT, security, legal, communications, and other teams across and outside of the organization must be involved."[26]

Third, keep the plan fresh – don't make it and forget it.[27] "You can't expect a professional sports team to know what to do on game day if they haven't been coached through the plays," says Andrew Hay, CISO at Data Gravity, Inc.[28] "An incident response activity should create muscle memory."[29]

Finally, stay the course when the event happens.[30] "Even the most sophisticated plan can implode when teams don't stick to the playbook. The plan can break down if incident response teams allow their emotions to guide their decisions."[31] Another threat to a well-honed plan is an organization's reluctance to enact the plan until it is too late.[32]

IV. Conclusion

Cyber Incident Response Plans are vital to quickly responding to a cyber incident. While the business environment concerning cybersecurity should start with the C-suite of the company, people from many levels and departments within the organization should be involved in the creation and implementation of the Cyber Incident Response Plan. The Plan should be easy to follow, updated regularly, and tested at least annually to practice and find weaknesses within the Plan. While the likelihood of a cyber-attack is high, if a company has a strong Cyber Incident Response Plan, it can easily and quickly mitigate the damage.

* Kalie is a J.D. Candidate at Elon University School of Law, graduating in December 2017. She received a B.S. in Business & Public Policy from Young Harris College in 2015.

[1] Matt Hamblen, *Privacy worries are on the rise, new poll of U.S. consumers shows*. Computerworld (Jan. 30, 2017), http://www.computerworld.com/article/3163207/data-privacy/privacy-worries-are-on-the-rise-new-poll-of-u-s-consumers-shows.html.

[2] *Id*.

[3] *See id. See also* Angie Mohr, *3 Ways Cyber-Crime Impacts Business*, Investopedia (Jan. 21, 2012), http://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx.

[4] Tucker Bailey, Josh Bradley & James Kaplan, *How good is your cyberincident-response plan?*, McKinsey & Co.: Digital McKinsey (Dec. 2013), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-good-is-your-cyberincident-response-plan.

[5] *Id*.

[6] *Id.*

[7] Carin Hughes, *4 Steps to A Strong Incident Response Plan*, CSO Online (Aug. 4, 2016), http://www.csoonline.com/article/3104203/techology-business/4-steps-to-a-strong-incident-response-plan.html.

[8] *Id*.

[9] Bailey, *supra* note 4.

[10] *Id*.

[11] *Id*.

[12] Michael Bartock et al, *Guide for Cybersecurity Event Recovery*, Nat'l Inst. of Standards and Tech. (June 2016), http://csrc.nist.gov/publications/drafts/800-184/sp800_184_draft.pdf.

[13] *Id.*

[14] *Id.*

[15] *See id.*

[16] *See id.*

[17] *See id.*

[18] Bailey*, supra* note 4.

[19] *See* Bartock, *supra* note 12.

[20] *See* Hughes, *supra* note 7.

[21] *Id.*

[22] *Id.*

[23] *Id*.

[24] *Id.*

[25] *Id.*

[26] *Id*.

[27] *Id.*

[28] *Id*.

[29] *Id*.

[30] *Id.*

[31] *Id*.

[32] *Id*.